一种强安全的无证书非交互密钥交换协议

魏 云 魏福山 马传贵
(解放军信息工程大学数学工程与先进计算国家重点实验室 郑州 450001)

摘 要 非交互密钥交换协议(Non-interactive Key Exchange,NIKE)允许通信双方在没有信息交互的情况下生成一个共享密钥。在基于身份的非交互密钥交换协议(Identity-based Non-interactive Key Exchange,ID-NIKE)中,用户私钥是由私钥生成中心(Private Key Generator,PKG)分发给用户的,因此PKG可以计算出用户之间的共享密钥,即存在密钥托管的问题。针对ID-NIKE的上述不足,基于无证书的公钥密码体制(Certificateless Public Key Cryptography,CL-PKC),首先提出了无证书非交互密钥交换协议的安全模型,然后设计了一个强安全的无证书非交互密钥交换协议方案,并在随机预言模型下基于BDH假设给出了协议的安全性证明。该方案是第一个基于CL-PKC的非交互密钥交换协议方案,并结合了CL-PKC和NIKE的优点,因此该方案不仅具有非交互的性质,而且PKG计算不出用户间的共享密钥,所以其可以更好地保护用户隐私。另外,该协议还允许用户部分秘密信息泄露,因此具有更高的安全性。

关键词 无证书公钥密码体制,非交互密钥交换协议,随机预言模型
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2014.12.022

Non-interactive Key Exchange Protocol Based on Certificateless Public Key Cryptography

WEI Yun WEI Fu-shan MA Chuan-gui
(State Key Laboratory of Mathematical Engineering and Advanced Computing,PLA Information Engineering University,Zhengzhou 450001,China)

Abstract A non-interactive key exchange (NIKE) allows two parties to establish a shared key without further communication. In ID-based non-interactive key exchange (ID-NIKE),PKG (private key generator) knows user's private key, so it can calculate the shared key between two participants,which is namely the key escrow problem. In this paper,the first security model for certificateless non-interactive key exchange was proposed. And then a scheme of a certificateless non-interactive key exchange was given. The new scheme is proven secure in the Random Oracle Model based on the hardness of the bilinear diffie-Hellman assumption (BDH). It is the first non-interactive key exchange scheme based on certificateless public key cryptography (CL-PKC),which combines the advantage of the CL-PKC and the NIKE. Thus the center cannot calculate the shared key,which solves the key escrow problem in ID-NIKE. Especially,our scheme allows partial private key leakage,so it is more secure than other related schemes.

Keywords Certificateless public key cryptography,Non-interactive key exchange,Random oracle model

1 引言

非交互密钥交换协议(Non-interactive Key Exchange,NIKE)允许通信双方在只知道对方公钥并且没有信息交互的情况下建立一个共享密钥。由于其非交互的特性,非交互密钥交换协议极大地减少了协议的通信轮数。在无线网络环境中,由于终端接收和发送信号所消耗的资源远远大于计算所消耗的资源,因此非交互的密钥交换协议特别适用于无线网络环境。另外,非交互密钥交换协议在节省计算资源的同时还减小了敌手攻击的可能性,提高了通信的安全。此外,非交互密钥交换协议还可以作为一个基本的密码学组件用于实现不可否认认证[1],构建交互的密钥交换协议[2]以及指定验证者的签名方案[3]。非交互密钥交换协议由于具有广泛的应用需求,因此受到了广大学者的关注,成为安全协议研究中的一个热点问题。

最早的非交互密钥交换协议可以追溯到经典的DH密钥交换协议[4]。如果我们将DH交换协议中的g^r和g^y分别看作用户Alice和Bob的公钥,那么DH协议就是一个典型的非交互密钥交换协议。当前,对非交互密钥交换协议的研究可以分为基于PKI的非交互密钥交换协议[5-8]和基于身份的非交互密钥交换协议[9-18]两类。2006年,Bernstein[5]设计了一个高效的椭圆曲线上的非交互密钥交换协议,并定义了一个基于PKI的非交互密钥交换协议的安全模型。随后,Cash等人[6]又提出了一个更强的非交互密钥交换协议的安全模

到稿日期:2014-01-09 返修日期:2014-03-14 本文受到国家自然科学基金(61379150,61309016),河南省自然科学基金(122102210426),信息保障技术重点实验室开放课题(KJ-13-02),"十二五"密码发展基金(MMJJ201201005)资助。
魏 云(1988—),女,硕士生,主要研究方向为密码协议,E-mail:weiyuntail88@sian.com;魏福山(1983—),男,博士,讲师,主要研究方向为密码协议;马传贵(1962—),男,博士生导师,CCF会员,主要研究方向为密码协议。

型，并且在随机预言模型下分析了基于孪生 Diffie-Hellman 的非交互密钥交换协议的安全性。2013 年 Freire 等人[7]系统地分析了基于 PKI 的非交互密钥交换协议安全模型之间的关系，并研究了随机预言模型和标准模型下基于 PKI 的非交互密钥交换协议的构造。

在基于身份的非交互密钥交换协议的研究方面，Maurer 和 Yacobi[9]在 1992 年基于 $(\mathbb{Z}/m\mathbb{Z})^*$ 上的离散对数构造了第一个基于身份的非交互密钥分发协议；该协议中用到了带陷门的模幂单向函数，要求计算模 m 的离散对数对于可信中心是可行的，而对于不知道 m 分解因子的敌手则是不可行的。但是很快 Lim 等人[10]指出他们的协议中存在两个不足：首先平方法容易使 m 泄露；其次，中心计算用户私钥需要很大的计算能力。后来 Maurer 和 Yacobi[11]对该协议进行了改进，然而在改进之后的协议中，两个用户合谋就可以获取中心的秘密信息(即模数 m 的分解)[12]。2000 年，Sakai 等人[13]首次将椭圆曲线上的双线性对应用到基于身份的非交互密钥交换协议中。然而上述基于身份的非交互密钥交换协议都没有给出正式的安全性证明，直到 2006 年，Dupont 和 Enge[14]提出了一个基于身份的非交互密钥交换协议的安全模型，并将 Sakai 等人[13]的协议扩展到了一般的双线性对上。后来 Paterson 和 Srinivasan[15]又结合 Dupont 和 Enge 的安全模型[14]和交互的密钥交换协议的安全模型，提出了一个更强的安全模型，并证明了 Sakai 等人的协议在该模型下的安全性。他们还基于陷门离散对数群，构建了一个安全的基于身份的非交互密钥交换协议。2013 年，Wu 等人[19]又提出了一种基于自验证公钥密码体制(Self-certified Public Key Cryptography，Self-Certified PKC)的非交互认证密钥交换协议。

在基于身份的非交互密钥交换协议中，用户的公钥为用户的身份，用户的私钥是由私钥生成中心(Private Key Generator，PKG)分发给用户的，因此 PKG 知道用户的私钥，也可以计算出用户之间的共享密钥。针对基于身份的非交互密钥交换协议的这一不足，本文首先提出了基于无证书公钥密码体制的非交互密钥交换协议的概念，刻画了无证书非交互密钥交换协议的安全模型，然后利用双线性对构造了一种无证书非交互密钥交换协议方案，并在随机预言模型下基于 BDH 假设给出了该方案的安全性证明。我们的方案具有以下两点优势：首先，方案解决了基于身份的非交互密钥交换协议的密钥托管问题；其次，我们的协议可以抵抗无证书公钥密码体制中两类敌手的攻击，允许部分秘密信息泄露，因此比已有的方案具有更高的安全性。

2 无证书非交互密钥交换协议安全模型

本节首先给出了无证书非交互密钥交换协议的定义，然后描述了无证书非交互密钥交换协议的安全模型。

2.1 无证书非交互密钥交换协议的定义

一个无证书非交互密钥交换协议一般是由如下 6 个算法组成：

(1)系统建立阶段(Setup)：该算法是一个概率多项式时间算法，由 KGC 执行。输入安全参数 k，输出主密钥 msk 和系统公开参数 $params$。

(2)用户密钥生成阶段：

(2.1)部分密钥提取(PartialKeyExtract)：该算法由 KGC 执行。输入主密钥 msk 和系统公开参数 $params$ 以及用户 U_i 的身份 ID_i，算法输出该用户的部分私钥 D_i 和部分公钥 P_i，KGC 将部分密钥 (P_i, D_i) 通过安全信道传送给用户；

(2.2)设置秘密值(SetSecretValue)：该算法是一个概率多项式时间算法，由用户执行。输入系统公开参数 $params$ 以及用户 U_i 的身份 ID_i，输出用户的秘密值 s_i；

(2.3)设置私钥(SetPrivateKey)：该算法是一个确定性多项式时间算法，由用户执行。输入系统公开参数 $params$、用户 U_i 的身份 ID_i、用户的部分私钥 D_i 以及用户的秘密值 s_i，输出用户的私钥 SK_i；

(2.4)设置公钥(SetPublicKey)：该算法是一个确定性多项式时间算法，由用户执行。输入系统公开参数 $params$、用户 U_i 的身份 ID、用户的部分公钥 P_i 以及用户的秘密值 s_i，输出用户的公钥 PK_i。

(3)密钥共享阶段(SharedKey)：该算法是一个确定性多项式时间算法，由用户执行。输入系统公开参数 $params$、用户 U_1 的私钥 SK_1 和用户 U_2 的公钥 PK_2(或者用户 U_2 的私钥 SK_2 和用户 U_1 的公钥 PK_1)，输出用户 U_1 和 U_2 的共享密钥 $K_{1,2}$。

2.2 无证书非交互密钥交换协议安全模型

无证书密码体制中考虑两类敌手 $\mathcal{A}_\mathrm{I}$ 和 $\mathcal{A}_\mathrm{II}$：$\mathcal{A}_\mathrm{I}$ 表示第一类敌手，可以任意替换用户公钥，但不拥有主密钥；$\mathcal{A}_\mathrm{II}$ 表示第二类敌手，拥有主密钥但不可以替换用户公钥。基于这两种敌手类型，我们给出无证书非交互密钥交换协议的安全模型。模型由两个攻击游戏——“游戏 1”和“游戏 2”组成，两类敌手在其相应的游戏中分别与挑战者进行攻击游戏。具体游戏如下：

游戏 1：这是敌手 $\mathcal{A}_\mathrm{I}$ 与挑战者 $\mathcal{C}_\mathrm{I}$ 的游戏。

(1)系统建立阶段：$\mathcal{C}_\mathrm{I}$ 运行协议中 Setup 算法获得主密钥 msk 和系统公开参数 $params$，然后将 $params$ 发送给 $\mathcal{A}_\mathrm{I}$，而对主密钥 msk 严格保密。

(2)询问阶段：在这一阶段敌手 $\mathcal{A}_\mathrm{I}$ 可以进行以下询问，$\mathcal{C}_\mathrm{I}$ 模拟协议中相应算法并分别做出回答：

• PartialKeyExtract(ID)询问：$\mathcal{C}_\mathrm{I}$ 在收到询问之后，计算 $(P_{ID}, D_{ID}) = PartialKeyExtract(Params, msk, ID)$，并将结果返回给 $\mathcal{A}_\mathrm{I}$。

• PublicKeyExtract(ID)询问：在接收到此询问之后，挑战者先查询应答记录中该 ID 对应的部分私钥，若不存在，则先计算 $(P_{ID}, D_{ID}) = PartialKeyExtract(Params, msk, ID)$。接着运行 $SetSecretValue(Params, ID)$ 得到 s_{ID}，最后计算 $PK_{ID} = SetPublicKey(Params, ID, P_{ID}, s_{ID})$，将 PK_{ID} 返回给敌手。

• SecretValueExtract(ID)询问：对这种询问，若 ID 的公钥已被替换，则不对该询问作出回应；否则，$\mathcal{C}_\mathrm{I}$ 先查询记录中是否存在被询问 ID 的秘密值。如果存在，则直接将秘密值返回给敌手；否则，运行 SetSecretValue，得到用户的秘密值 s_{ID}，记录并将秘密值返回给 $\mathcal{A}_\mathrm{I}$。

• PrivateKeyExtract(ID_I)询问：$\mathcal{C}_\mathrm{I}$ 在收到此询问后，先

查询应答记录中是否有被询问 ID 的部分私钥，如果没有就先计算 $(P_{ID}, D_{ID}) = PartialKeyExtract(Params, msk, ID)$。接着运行 $SetSecretValue(Params, ID)$ 得到 s_{ID}，最后计算 $SK_{ID} = SetPrivateKey(Params, ID, D_{ID}, s_{ID})$，将 SK_{ID} 发给敌手 $\mathcal{A}_{\mathrm{I}}$。

• PublicKeyReplace(ID, PK_{ID})询问：敌手可以将用户的公钥替换成任意值，挑战者记录下最新替换的公钥。

• Reveal(ID_A, ID_B)询问：$\mathcal{C}_{\mathrm{I}}$ 通过查询应答记录或计算得到 SK_A 和 PK_B，然后计算 $K_{A,B} = SharedKey(params, SK_A, PK_B)$，将结果返回给 $\mathcal{A}_{\mathrm{I}}$。

(3)测试阶段：在这一阶段，敌手 $\mathcal{A}_{\mathrm{I}}$ 选择(ID_1, ID_2)，将其发给 $\mathcal{C}_{\mathrm{I}}$ 进行测试询问。挑战者先模拟协议中计算共享密钥的步骤计算 $K_{1,2}$。然后选择 $b \in \{0,1\}$，如果 $b=0$，将 $K_{1,2}$ 返回给 $\mathcal{A}_{\mathrm{I}}$；否则选择一个随机值返回给 $\mathcal{A}_{\mathrm{I}}$。

(4)猜测阶段：在这一阶段，敌手 $\mathcal{A}_{\mathrm{I}}$ 猜测 b'，若 $b'=b$，则敌手 $\mathcal{A}_{\mathrm{I}}$ 成功；否则，敌手 $\mathcal{A}_{\mathrm{I}}$ 失败。

为避免敌手 $\mathcal{A}_{\mathrm{I}}$ 在游戏中获得测试阶段 ID_1 或 ID_2 的全部秘密信息从而频繁地成功，故在上述询问和测试阶段中对敌手 $\mathcal{A}_{\mathrm{I}}$ 作如下限制：

(1)不可对测试阶段的 ID_1 或 ID_2 进行私钥询问；

(2)不可对测试阶段的 ID_1 或 ID_2 既进行部分密钥询问又替换其公钥；

(3)不可对测试阶段的 ID_1 或 ID_2 既进行部分密钥询问又进行秘密值询问；

(4)不可对测试阶段的(ID_1, ID_2)进行共享密钥询问。

游戏 2：这是敌手 $\mathcal{A}_{\mathrm{II}}$ 与挑战者 $\mathcal{C}_{\mathrm{II}}$ 的攻击游戏。

(1)系统建立阶段：$\mathcal{C}_{\mathrm{II}}$ 运行 Setup 获得主密钥 msk 和系统公开参数 $params$，然后将 $params$ 和主密钥 msk 发送给 $\mathcal{A}_{\mathrm{II}}$。

(2)询问阶段：由于 $\mathcal{A}_{\mathrm{II}}$ 拥有主密钥 msk，可以自己计算用户的部分密钥 $(P_{ID}, D_{ID}) = PartialKeyExtract(Params, msk, ID)$。那么在这一阶段中敌手 $\mathcal{A}_{\mathrm{II}}$ 可以进行以下询问，$\mathcal{C}_{\mathrm{II}}$ 模拟协议中相应算法分别作出回答。

• PublicKeyExtract(ID)询问：在接收到这一类询问之后，挑战者先查询应答记录中该 ID 对应的部分私钥，若不存在，则先计算 $(P_{ID}, D_{ID}) = PartialKeyExtract(Params, msk, ID)$。接着运行 $SetSecretValue(Params, ID)$ 得到 s_{ID}，最后计算 $PK_{ID} = SetPublicKey(Params, ID, P_{ID}, s_{ID})$，将结果返回给敌手 $\mathcal{A}_{\mathrm{II}}$。

• SecretValueExtract(ID)询问：$\mathcal{C}_{\mathrm{II}}$ 在收到此询问后，先查询记录中是否存在被询问 ID 的秘密值。如果存在，直接将秘密值返回给敌手；否则，运行 SetSecretValue，得到用户的秘密值 s_{ID}，记录并将秘密值返回给 $\mathcal{A}_{\mathrm{II}}$。

• PrivateKeyExtract(ID)询问：对于此询问，$\mathcal{C}_{\mathrm{II}}$ 先查询应答记录中是否有被询问 ID 的部分私钥，如果没有，就先计算 $(P_{ID}, D_{ID}) = PartialKeyExtract(Params, msk, ID)$。接着运行 $SetSecretValue(Params, ID)$ 得到 s_{ID}。最后计算 $SK_{ID} = SetPrivateKey(Params, ID, D_{ID}, s_{ID})$，将 SK_{ID} 发给敌手 $\mathcal{A}_{\mathrm{II}}$。

• Reveal(ID_A, ID_B)询问：$\mathcal{C}_{\mathrm{II}}$ 通过查询应答记录或计算得到 SK_A 和 PK_B，然后计算 $K_{A,B} = SharedKey(params, SK_A, PK_B)$，将结果返回给 $\mathcal{A}_{\mathrm{II}}$。

(3)测试阶段：在这一阶段，敌手 $\mathcal{A}_{\mathrm{II}}$ 选择(ID_1, ID_2)，将其发给 $\mathcal{C}_{\mathrm{II}}$ 进行测试询问。挑战者用类似于共享密钥询问的步骤计算出 $K_{1,2}$。选择 $b \in \{0,1\}$，如果 $b=0$，将 $K_{1,2}$ 返回给 $\mathcal{A}_{\mathrm{II}}$；否则随机选择一个值返回给 $\mathcal{A}_{\mathrm{II}}$。

(4)猜测阶段：在这一阶段，敌手 $\mathcal{A}_{\mathrm{II}}$ 猜测 b'，若 $b'=b$，则敌手 $\mathcal{A}_{\mathrm{II}}$ 成功；否则，敌手 $\mathcal{A}_{\mathrm{II}}$ 失败。

同样，在上述询问和测试阶段中，对敌手 $\mathcal{A}_{\mathrm{II}}$ 作如下限制：

(1)不可对测试阶段的 ID_1 或 ID_2 进行私钥询问；

(2)不可对测试阶段的 ID_1 或 ID_2 进行秘密值询问；

(3)不可对测试阶段的(ID_1, ID_2)进行共享密钥询问。

敌手 $\mathcal{A}_i$ 在游戏 i 中的优势定义为 $Adv(\mathcal{A}_i) = \Pr[b'=b] - 1/2, i \in \{I, II\}$。一个无证书非交互密钥交换协议是安全的，当且仅当不存在多项式时间的敌手可以以不可忽略的优势赢得上述游戏。

3 无证书非交互密钥交换协议方案

本节将给出一种无证书非交互密钥交换协议方案，具体如下：

(1)系统建立阶段：设 k 是安全参数，$e: G \times G \to G_T$ 是双线性映射，其中 G 和 G_T 是两个阶为素数 q 的循环群，$P \in G$ 是群 G 的一个生成元。KGC 随机选取主密钥 $s \in \mathbb{Z}_q^*$ 并计算 $P_0 = sP$。选择 hash 函数：$H_1: \{0,1\}^* \to G^*$，$H_2: G_T^* \times G^* \times G_T^* \to \{0,1\}^l$。系统公开参数 $params = \{q, G, G_T, e, P, P_0, H_1, H_2, l\}$，主密钥 $msk = s$。

(2)用户密钥生成阶段：

(2.1)部分密钥提取：输入用户的身份 ID 后，KGC 计算 $P_{ID} = H_1(ID)$，$D_{ID} = sP_{ID}$。KGC 返回用户的部分密钥(P_{ID}, D_{ID})；

(2.2)设置秘密值：用户随机选取 $x \in \mathbb{Z}_q^*$ 并输出 $s_{ID} = x$ 作为用户的秘密值；

(2.3)设置私钥：用户的私钥 $SK_{ID} = (s_{ID}, D_{ID}) = (x, sH_1(ID))$；

(2.4)设置公钥：用户的公钥 $PK_{ID} = (P_{ID}, T_{ID}) = (H_1(ID), xP)$。

(3)计算共享密钥阶段：A 计算 $K_1 = e(s_A P_0 + D_A, P_B + T_B)$，$K_2 = s_A T_B$，$K_3 = e(D_A, P_B)$，最后计算 $K_{A,B} = H_2(K_1, K_2, K_3)$；

B 计算 $K_1' = e(P_A + T_A, s_B P_0 + D_B)$，$K_2' = s_B T_A$，$K_3' = e(P_A, D_B)$，最后计算 $K_{A,B}' = H_2(K_1, K_2, K_3)$。显然 $K_{A,B} = K_{A,B}'$。

4 方案的安全性证明

定理 1 如果 BDH 假设在 (G, G_T, e, P) 上成立，并且 CDH 假设在 (G, P) 上成立，那么本文提出的方案在随机预言模型下是安全的。

要证明该定理，我们需要证明两个引理。引理 1 和引理 2 分别表明我们的方案对于敌手 $\mathcal{A}_{\mathrm{I}}$ 和 $\mathcal{A}_{\mathrm{II}}$ 是安全的，由于第一类敌手 $\mathcal{A}_{\mathrm{I}}$ 具有替换公钥的能力，这一能力使得敌手可以将用户的秘密值替换成为自己所选的任意值，强于秘密值询问的能力，因此，在敌手 $\mathcal{A}_{\mathrm{I}}$ 的攻击游戏模拟中，不对秘密值询问进

行模拟。

引理 1 在随机预言模型下，假设存在第一类敌手 $\mathcal{A}_1$ 在 $t_{\mathcal{A}_1}$ 时间内，至多作 q_1 条对 H_1 的询问和 q_2 条对 H_2 的询问后，可以破坏本文提出的协议，则存在算法 $\mathcal{B}_I$ 在 $O(t_{\mathcal{A}_1})$ 时间内解决 BDH 困难问题，且有：

$$Adv_{\mathcal{B}_1}^{BDH} \geqslant Adv_{\mathcal{A}_1}(k)/(q_1^2 q_2)$$

证明：假设敌手 $\mathcal{A}_1$ 可以破坏本文提出的方案，接下来利用 $\mathcal{A}_1$ 构造算法 $\mathcal{B}_1$ 来解决 BDH 困难问题。$\mathcal{B}_I$ 的输入为一个 BDH 实例($U=uP, V=vP, W=wP$)，其中 $u,v,w\in\mathbb{Z}_q^*$，$U, V, W\in G$。$\mathcal{B}_I$ 的目的就是要计算 $e(P,P)^{uvw}$。为了得到结果，$\mathcal{B}_I$ 利用 $\mathcal{A}_1$ 作为子程序试图解决 BDH 困难问题，并且充当游戏中的挑战者。不妨假设 $\mathcal{A}_1$ 在测试阶段对(ID_1, ID_2)进行测试询问，分以下 4 种情形进行分析：

情形 1：敌手 $\mathcal{A}_1$ 对测试阶段的 ID_1 和 ID_2 进行了部分密钥询问(那么，$\mathcal{A}_1$ 不能再替换掉 ID_1、ID_2 的公钥)；

情形 2：敌手 $\mathcal{A}_1$ 替换了测试阶段的 ID_1 和 ID_2 的公钥(那么，$\mathcal{A}_1$ 不能再对测试阶段的 ID_1、ID_2 进行部分密钥询问)；

情形 3：敌手 $\mathcal{A}_1$ 对测试阶段的 ID_1 进行了部分密钥询问，并替换了 ID_2 的公钥(那么，$\mathcal{A}_1$ 不能再替换掉 ID_1 的公钥，也不能对 ID_2 进行部分密钥询问)；

情形 4：敌手 $\mathcal{A}_1$ 替换了 ID_1 的公钥，并对测试阶段的 ID_2 进行了部分密钥询问(那么，$\mathcal{A}_1$ 不能再替换掉 ID_2 的公钥，也不能对 ID_1 进行部分密钥询问)。

以上 4 种情形中，第三种情形和第四种情形可以看作同一种情形，即敌手 $\mathcal{A}_1$ 替换了测试阶段中 ID_i 的公钥，并对测试阶段的另一用户的部分密钥进了行询问。

4.1 对情形 1 的分析

首先 $\mathcal{B}_I$ 设 $P_0=W=wP$(即系统主密钥设为 w，但是 $\mathcal{B}_I$ 不知道 w)，系统参数 $params=\{q, G, G_T, e, P, P_0=W=wP, H_1, H_2, l\}$，将 $params$ 发给敌手 $\mathcal{A}_1$，$\mathcal{B}_I$ 随机选取 $M, N\in\{1, 2, \cdots, q_1\}$($\mathcal{B}_1$ 猜测敌手 $\mathcal{A}_1$ 会对(ID_M, ID_N)进行测试询问，只有猜测正确，$\mathcal{B}_1$ 才可能成功解决 BDH 困难问题)。$\mathcal{A}_1$ 进行一系列的询问，$\mathcal{B}_1$ 作出如下应答：

(1)H_1 询问：$\mathcal{B}_1$ 用表 L_1 来记录 $\mathcal{A}_1$ 对 H_1 的询问，表中每一项的格式为($ID, d_{ID}, d_{ID}P$)，表 L_1 初始化为空(本文证明中所有表都被初始化为空)。如果表 L_1 中已存在表项($ID, d_{ID}, d_{ID}P$)(这样，虽然 $\mathcal{B}_1$ 不知道系统主密钥，但是 ID 的部分私钥 $\mathcal{B}_1$ 还是可以计算的，如 $D_{ID}=wP_{ID}=wd_{ID}P=d_{ID}(wP)=d_{ID}W$)，则 $\mathcal{B}_1$ 将 $d_{ID}P$ 返回给 $\mathcal{A}_1$；若不存在，则随机选取 $d_{ID}\in\mathbb{Z}_q^*$，将($ID, d_{ID}, d_{ID}P$)存入 L_1 中，并将 $d_{ID}P$ 返回给 $\mathcal{A}_1$。

(2)H_2 询问：$\mathcal{B}_1$ 用表 L_2 来记录 $\mathcal{A}_1$ 对 H_2 的询问。如果表 L_2 中已存在表项(K_1, K_2, K_3, K)，则 $\mathcal{B}_1$ 将 K 返回给 $\mathcal{A}_1$；若不存在，则随机选取 $K\in\{0,1\}^l$，将(K_1, K_2, K_3, K)存入 L_2 中，并将 K 返回给 $\mathcal{A}_1$。

(3)部分密钥询问：$\mathcal{B}_1$ 用表 L_{pak} 来记录 $\mathcal{A}_1$ 对部分密钥的询问。先查询表 L_{pk}，若其中 ID 对应的表项为(ID,(P_{ID}, T_{ID}),$\perp$)(文中符号 $\perp$ 表示该值未知，此处(ID,(P_{ID}, T_{ID}), $\perp$)，表示敌手已经替换过 ID 的公钥，则敌手不能再询问其部分密钥)，则 $\mathcal{B}_1$ 退出。否则，查询表 L_{pak}，如果表 L_{pak} 中已存在表项(ID, P_{ID}, D_{ID})，则 $\mathcal{B}_1$ 将(P_{ID}, D_{ID})返回给 $\mathcal{A}_1$；若不存在，则计算 $P_{ID}=H_1(ID)=d_{ID}P$，$D_{ID}=d_{ID}W=d_{ID}(wP)$，将($ID, P_{ID}, D_{ID}$)存入 L_{pak} 中，并将(P_{ID}, D_{ID})返回给 $\mathcal{A}_1$。

(4)公钥询问：$\mathcal{B}_1$ 用表 L_{pk} 来记录用户的公私钥对。如果表 L_{pk} 中已存在表项(ID,(P_{ID}, T_{ID}),·)(文中用符号·表示该处既可以为已知值，也可为 $\perp$)，则 $\mathcal{B}_1$ 将(P_{ID}, T_{ID})返回给 $\mathcal{A}_1$；若不存在，则分为如下 3 种情况进行应答：

· 若 $ID\notin\{ID_M, ID_N\}$，则如上运行部分密钥提取得到(P_{ID}, D_{ID})，然后随机选取 $s_{ID}\in\mathbb{Z}_q^*$，计算 $T_{ID}=s_{ID}P$，将(ID,(P_{ID}, T_{ID}),(s_{ID}, D_{ID}))存入 L_{pk} 中，并将(P_{ID}, T_{ID})返回给 $\mathcal{A}_1$；

· 若 $ID=ID_M$，则如上运行部分密钥提取得到(P_M, D_M)，令 $T_M=U=uP$(这样，ID_M 的秘密值为 u，且 $\mathcal{B}_1$ 不知道该值)，将(ID_M,(P_M, T_M),($\perp, D_M$))存入 L_{pk} 中，并将(P_M, T_M)返回给 $\mathcal{A}_1$；

· 若 $ID=ID_N$，则如上运行部分密钥提取得到(P_N, D_N)，计算 $T_N=V=vP$(这样，ID_N 的秘密值为 v，且 $\mathcal{B}_I$ 不知道该值)，将(ID_N,(P_N, T_N),($\perp, D_N$))存入 L_{pk} 中，并将(P_N, T_N)返回给 $\mathcal{A}_1$。

(5)私钥询问：若 $ID\in\{ID_M, ID_N\}$，则 $\mathcal{B}_1$ 退出；否则，如果表 L_{pk} 中不存在表项(ID,(P_{ID}, T_{ID}),(s_{ID}, D_{ID}))，则先如上运行公钥询问，然后在 L_{pk} 中查询 ID 的私钥(s_{ID}, D_{ID})，并将(s_{ID}, D_{ID})返回给 $\mathcal{A}_1$。

(6)公钥替换：敌手 $\mathcal{A}_1$ 可以将用户的公钥替换成为自己挑选的值，$\mathcal{B}_1$ 记录下替换的公钥值(P_{ID}', T_{ID}')，将 L_{pk} 中 ID 对应的表项替换成(ID,(P_{ID}', T_{ID}'),$\perp$)。

(7)共享密钥询问：若(ID_A, ID_B)=(ID_M, ID_N)，则 $\mathcal{B}_1$ 退出；否则，有$|\{ID_A, ID_B\}\cap\{ID_M, ID_N\}|\leqslant 1$，不妨假设 $ID_A\notin\{ID_M, ID_N\}$，那么查询 L_{pk} 找到 ID_A 的私钥或通过私钥提取计算出 ID_A 的私钥(s_A, D_A)，再通过查询或计算得到 ID_A 和 ID_B 的公钥(P_A, T_A)、(P_B, T_B)，然后计算 $K_{A,B}$，记录($ID_A, ID_B, K_{A,B}$)，并将 $K_{A,B}$ 返回给 $\mathcal{A}_1$。

(8)测试询问：$\mathcal{A}_1$ 选取一对(ID_1, ID_2)进行测试询问。如果(ID_1, ID_2)$\neq$(ID_M, ID_N)(即 $\mathcal{B}_1$ 猜测错误)，则 $\mathcal{B}_1$ 退出并且失败；否则，$\mathcal{B}_1$ 随机选择 $K_{1,2}'\in\{0,1\}^l$，并将 $K_{1,2}'$ 发送给 $\mathcal{A}_1$。

至此，$\mathcal{B}_1$ 的模拟结束。若 $\mathcal{A}_1$ 输出 $b'=1$，则 $\mathcal{B}_1$ 从 L_2 中随机选取(K_1, K_2, K_3)，$\mathcal{B}_1$ 计算：

$$S=K_1/[e(h_A d_A W, h_B d_B P+V)\cdot e(W, h_B d_B U)]=e(P,P)^{uvw}$$

最后，$\mathcal{B}_1$ 输出 S；否则，输出随机值。

下面我们分析 $\mathcal{B}_1$ 的优势。

设 $\mathcal{F}$ 表示事件“$\mathcal{B}_1$ 在模拟过程中不退出”，则 $\Pr[\mathcal{F}]\geqslant 1/q_1^2$。又如果 $\mathcal{A}_1$ 输出 $b'=1$(即 $\mathcal{A}_1$ 攻击成功)，则 $\mathcal{A}_1$ 对正确的(K_1, K_2, K_3)进行过 H_3 询问，其中 $K_1=e(s_A P_0+h_A D_A, h_B P_B+T_B)=e(uwP+h_A d_A wP, h_B d_B P+vP)$，那么 $\mathcal{B}_I$ 可以以 $1/q_2$ 的概率得到正确的(K_1, K_2, K_3)。综上，如果 $\mathcal{B}_1$ 在模拟过程中不退出，且 $\mathcal{A}_1$ 对(K_1, K_2, K_3)进行过 H_3 询问也就可以通过如上计算出 $e(P,P)^{uvw}$，即解决 BDH 困难问题，且

$$Adv_{\mathcal{B}_1}^{BDH}=\Pr[\mathcal{F}]\cdot Adv_{\mathcal{A}_1}(k)/q_2\geqslant Adv_{\mathcal{A}_1}(k)/q_1^2 q_2$$

4.2 对情形 2 的分析

首先 $\mathcal{B}_I$ 令 $params=\{q,G,G_T,e,P,P_0=W=wP,H_1,H_2,l\}$，将 $params$ 发给敌手 $\mathcal{A}_I$，$\mathcal{B}_I$ 随机选取 $M,N\in\{1,2,\cdots,q_1\}$。$\mathcal{A}_I$进行一系列的询问，$\mathcal{B}_I$ 作出如下应答：

(1)H_1 询问：$\mathcal{B}_I$ 用表 L_1 来记录 $\mathcal{A}_I$对 H_1 的询问。如果表 L_1 中已存在表项$(ID,d_{ID},d_{ID}P)$，则 $\mathcal{B}_I$ 将 $d_{ID}P$ 返回给 $\mathcal{A}_I$；若不存在，且 $ID\notin\{ID_M,ID_N\}$，则随机选取 $d_{ID}\in\mathbb{Z}_q^*$，将$(ID,d_{ID},d_{ID}P)$存入 L_1 中，并将 $d_{ID}P$ 返回给 $\mathcal{A}_I$；否则若 $ID=ID_M$，则将$(ID,\perp,U=uP)$存入 L_1 中，并返回 U；若 $ID=ID_N$，则将$(ID,\perp,V=vP)$存入 L_1 中，并返回 V。

(2)H_2 询问：$\mathcal{B}_I$ 用表 L_2 来记录 $\mathcal{A}_I$对 H_2 的询问。如果表 L_2 中已存在表项(K_1,K_2,K_3,K)，则 $\mathcal{B}_I$ 将 K 返回给 $\mathcal{A}_I$；若不存在，则随机选取 $K\in\{0,1\}^l$，将(K_1,K_2,K_3,K)存入 L_2 中，并将 K 返回给 $\mathcal{A}_I$。

(3)部分密钥询问：$\mathcal{B}_I$ 用表 L_{puk} 来记录 $\mathcal{A}_I$对部分密钥的询问。先查询表 L_{pk}，若其中 ID 对应的表项为$(ID,(P_{ID},T_{ID}),\perp)$，则 $\mathcal{B}_I$ 退出。否则，查询表 L_{puk}，如果表 L_{puk} 中已存在表项(ID,P_{ID},D_{ID})，则 $\mathcal{B}_I$ 将(P_{ID},D_{ID})返回给 $\mathcal{A}_I$；若不存在且 $ID\notin\{ID_M,ID_N\}$，则计算 $P_{ID}=H_1(ID)=d_{ID}P$，$D_{ID}=d_{ID}W=d_{ID}(wP)$，将$(ID,P_{ID},D_{ID})$存入 L_{puk} 中，并将(P_{ID},D_{ID})返回给 $\mathcal{A}_I$；否则，$\mathcal{B}_I$ 退出。

(4)公钥询问：$\mathcal{B}_I$ 用表 L_{pk} 来记录用户的公私钥对。如果表 L_{pk} 中已存在表项$(ID,(P_{ID},T_{ID}),\cdot)$，则 $\mathcal{B}_I$ 将(P_{ID},T_{ID})返回给 $\mathcal{A}_I$；若不存在，则如上运行部分密钥提取得到(P_{ID},D_{ID})，然后随机选取 $s_{ID}\in\mathbb{Z}_q^*$，计算 $T_{ID}=s_{ID}P$，将$(ID,(P_{ID},T_{ID}),(s_{ID},D_{ID}))$存入 L_{pk} 中，并将(P_{ID},T_{ID})返回给 $\mathcal{A}_I$；

(5)私钥询问：若 $ID\in\{ID_M,ID_N\}$，则 $\mathcal{B}_I$ 退出；否则，如果表 L_{pk} 中不存在表项$(ID,(P_{ID},T_{ID}),(s_{ID},D_{ID}))$，则先如上运行公钥询问，然后在 L_{pk} 查询 ID 的私钥(s_{ID},D_{ID})，并将(s_{ID},D_{ID})返回给 $\mathcal{A}_I$。

(6)公钥替换：敌手 $\mathcal{A}_I$可以将用户的公钥替换成为自己挑选的值，$\mathcal{B}_I$ 记录下替换的公钥值(P_{ID}',T_{ID}')，将 L_{pk} 中 ID 对应的表项替换成$(ID,(P_{ID}',T_{ID}'),\perp)$。由于公钥中的 $P_{ID}=H_1(ID)$是可以被检验的，因此敌手是不可以进行替换的。那么，不妨假设 $\mathcal{A}_I$将 ID_1 和 ID_2 的公钥替换为$(P_1,T_1'=x'P)$，$(P_2,T_2'=y'P)$。

(7)共享密钥询问：若$(ID_A,ID_B)=(ID_M,ID_N)$，则 $\mathcal{B}_I$ 退出；否则，有$|\{ID_A,ID_B\}\cap\{ID_M,ID_N\}|\leqslant 1$，不妨假设 $ID_A\notin\{ID_M,ID_N\}$，那么查询 L_{pk} 来找到 ID_A 的私钥或通过私钥提取来计算出 ID_A 的私钥(s_A,D_A)，公钥(P_A,T_A)，和 ID_B 的公钥(P_B,T_B)，然后计算 $K_{A,B}$，记录$(ID_A,ID_B,K_{A,B})$，并将 $K_{A,B}$返回给 $\mathcal{A}_I$。

(8)测试询问：$\mathcal{A}_I$选取一对(ID_1,ID_2)进行测试询问。如果$(ID_1,ID_2)\neq(ID_M,ID_N)$，则 $\mathcal{B}_I$ 退出并且失败；否则，$\mathcal{B}_I$ 随机选择 $K_{1,2}'\in\{0,1\}^l$，并将 $K_{1,2}'$发送给 $\mathcal{A}_I$。

至此，$\mathcal{B}_I$ 的模拟结束。$\mathcal{A}_I$若输出 $b'=1$，则 $\mathcal{B}_I$ 从 L_2 中随机选取(K_1,K_2,K_3)，$\mathcal{B}_I$ 输出 K_3。

下面分析 $\mathcal{B}_I$ 的优势。

设 $\mathcal{F}$ 表示事件“$\mathcal{B}_I$ 在模拟过程中不退出”，则 $\Pr[\mathcal{F}]\geqslant 1/q_1^2$。综上，如果 $\mathcal{B}_I$ 在模拟过程中不退出，且 $\mathcal{A}_I$对(K_1,K_2,K_3)进行过 H_3 询问，其中 $K_3=e(D_A,P_B)=e(uwP,vP)=e(P,P)^{uvw}$，那么 $\mathcal{B}_I$ 就可以以优势 $Adv_{\mathcal{A}_I}^{BDH}$解决 BDH 问题，且

$$Adv_{\mathcal{B}_I}^{BDH}=\Pr[\mathcal{F}]\cdot Adv_{\mathcal{A}_I}(k)/q_2\geqslant Adv_{\mathcal{A}_I}(k)/q_1^2q_2$$

4.3 对情形 3 的分析

首先 $\mathcal{B}_I$ 令 $params=\{q,G,G_T,e,P,P_0=W=wP,H_1,H_2,l\}$，将 $params$ 发给敌手 $\mathcal{A}_I$，$\mathcal{B}_I$ 随机选取 $M,N\in\{1,2,\cdots,q_1\}$。$\mathcal{A}_I$进行一系列的询问，$\mathcal{B}_I$ 作出如下应答：

(1)H_1 询问：$\mathcal{B}_I$ 用表 L_1 来记录 $\mathcal{A}_I$对 H_1 的询问。如果表 L_1 中已存在表项$(ID,d_{ID},d_{ID}P)$，则 $\mathcal{B}_I$ 将 $d_{ID}P$ 返回给 $\mathcal{A}_I$；若不存在，且 $ID\neq ID_M$，则随机选取 $d_{ID}\in\mathbb{Z}_q^*$，将$(ID,d_{ID},d_{ID}P)$存入 L_1 中，并将 $d_{ID}P$ 返回给 $\mathcal{A}_I$；否则若 $ID=ID_M$，则将$(ID_I,\perp,U=uP)$存入 L_1 中，并返回 U。

(2)H_2 询问：$\mathcal{B}_I$ 用表 L_2 来记录 $\mathcal{A}_I$对 H_2 的询问。如果表 L_2 中已存在表项(K_1,K_2,K_3,K)，则 $\mathcal{B}_I$ 将 K 返回给 $\mathcal{A}_I$；若不存在，则随机选取 $K\in\{0,1\}^l$，将(K_1,K_2,K_3,K)存入 L_2 中，并将 K 返回给 $\mathcal{A}_I$。

(3)部分密钥询问：$\mathcal{B}_I$ 用表 L_{puk} 来记录 $\mathcal{A}_I$对部分密钥的询问。先查询表 L_{pk}，若其中 ID 对应的表项为$(ID,(P_{ID},T_{ID}),\perp)$，则 $\mathcal{B}_I$ 退出。否则，查询表 L_{puk}，如果表 L_{puk} 中已存在表项(ID,P_{ID},D_{ID})，则 $\mathcal{B}_I$ 将(P_{ID},D_{ID})返回给 $\mathcal{A}_I$；若不存在，则计算 $P_{ID}=H_1(ID)=d_{ID}P$，$D_{ID}=d_{ID}W=d_{ID}(wP)$，将$(ID,P_{ID},D_{ID})$存入 L_{puk} 中，并将(P_{ID},D_{ID})返回给 $\mathcal{A}_I$。

(4)公钥询问：$\mathcal{B}_I$ 用表 L_{pk} 来记录用户的公私钥对。如果表 L_{pk} 中已存在表项$(ID,(P_{ID},T_{ID}),\cdot)$，则 $\mathcal{B}_I$ 将(P_{ID},T_{ID})返回给 $\mathcal{A}_I$；若不存在，且 $ID\neq ID_N$，则如上运行部分密钥来提取得到(P_{ID},D_{ID})，然后随机选取 $s_{ID}\in\mathbb{Z}_q^*$，计算 $T_{ID}=s_{ID}P$，将$(ID,(P_{ID},T_{ID}),(s_{ID},D_{ID}))$存入 L_{pk} 中，并将(P_{ID},T_{ID})返回给 $\mathcal{A}_I$；否则，若 $ID=ID_N$，则将$(ID,(P_B=d_BP,T_B=V=vP),(\perp,D_B=d_B(wP)))$存入 L_{pk} 中，并将(P_B,T_B)返回给 $\mathcal{A}_I$。

(5)私钥询问：若 $ID\in\{ID_M,ID_N\}$，则 $\mathcal{B}_I$ 退出；否则，如果表 L_{pk} 中不存在表项$(ID,(P_{ID},T_{ID}),(s_{ID},D_{ID}))$，则先如上运行公钥询问，然后在 L_{pk} 中查询 ID 的私钥(s_{ID},D_{ID})，并将(s_{ID},D_{ID})返回给 $\mathcal{A}_I$。

(6)公钥替换：敌手 $\mathcal{A}_I$可以将用户的公钥替换成为自己挑选的值，$\mathcal{B}_I$ 记录下替换的公钥值(P_{ID}',T_{ID}')，将 L_{pk} 中 ID 对应的表项替换成$(ID,(P_{ID}',T_{ID}'),\perp)$。由于公钥中的 $P_{ID}=H_1(ID)$是可以被检验的，因此敌手是不可以进行替换的。那么，不妨假设 $\mathcal{A}_I$将 ID_1 的公钥替换为$(P_1,T_1'=x'P)$。

(7)共享密钥询问：若$(ID_A,ID_B)=(ID_M,ID_N)$，则 $\mathcal{B}_I$ 退出；否则，有$|\{ID_A,ID_B\}\cap\{ID_M,ID_N\}|\leqslant 1$，不妨假设 $ID_A\notin\{ID_M,ID_N\}$，那么查询 L_{pk} 找到 ID_A 的私钥或通过私钥提取计算出 ID_A 的私钥(s_A,D_A)，公钥(P_A,T_A)，和 ID_B 的公钥(P_B,T_B)，然后计算 $K_{A,B}$，记录$(ID_A,ID_B,K_{A,B})$，并将 $K_{A,B}$返回给 $\mathcal{A}_I$。

(8)测试询问：$\mathcal{A}_I$选取一对(ID_1,ID_2)进行测试询问。如果$(ID_1,ID_2)\neq(ID_M,ID_N)$，则 $\mathcal{B}_I$ 退出并且失败；否则，$\mathcal{B}_I$ 随机选择 $K_{1,2}'\in\{0,1\}^l$，并将 $K_{1,2}'$发送给 $\mathcal{A}_I$。

至此，$\mathcal{B}_I$ 的模拟结束。$\mathcal{A}_I$若输出 $b'=1$，则 $\mathcal{B}_I$ 从 L_2 中随机选取(K_1,K_2,K_3)，$\mathcal{B}_I$ 计算 $S=K_1/[e(P_0,T_A+h_AP_A)^{h_Bd_B}$

$\cdot e(P_0,K_2)]$，最后，$\mathcal{B}_{\mathrm{I}}$ 输出 $S^{h_A^{-1}}$。

下面分析 $\mathcal{B}_{\mathrm{I}}$ 的优势。

设 $\mathcal{F}$ 表示事件“$\mathcal{B}_{\mathrm{I}}$ 在模拟过程中不退出”，则 $\Pr[\mathcal{F}]\geqslant 1/q_1^2$。综上，如果 $\mathcal{B}_{\mathrm{I}}$ 在模拟过程中不退出，且 $\mathcal{A}_{\mathrm{I}}$ 对 (K_1,K_2,K_3) 进行过 H_3 询问，其中 $K_1=e(s_AP_0+h_AD_A,h_BP_B+T_B)=e(x'wP+h_AwuP,h_Bd_BP+vP)$，$K_2=s_AT_B=x'vP$，那么 $\mathcal{B}_{\mathrm{I}}$ 就可以以优势 $Adv_{\mathcal{B}_{\mathrm{I}}}^{BDH}$ 解决 BDH 问题，即

$$Adv_{\mathcal{B}_{\mathrm{I}}}^{BDH}=\Pr[\mathcal{F}]\cdot Adv_{\mathcal{A}_{\mathrm{I}}}(k)/q_2\geqslant Adv_{\mathcal{A}_{\mathrm{I}}}(k)/q_1^2q_2$$

4.4 对第二类敌手的分析

引理 2 假设在随机预言模型下，存在第二类敌手 $\mathcal{A}_{\mathrm{II}}$ 在 $t_{\mathcal{A}_{\mathrm{II}}}$ 时间内，至多进行 q_1 条对 H_1 的询问和 q_2 条对 H_2 的询问后可以破坏本文提出的方案，则存在敌手 $\mathcal{B}_{II}$ 可以在 $O(t_{\mathcal{A}_{\mathrm{II}}})$ 时间内解决 CDH 困难问题，且有：

$$Adv_{\mathcal{A}_{\mathrm{II}}}^{CDH}\geqslant Adv_{\mathcal{A}_{\mathrm{II}}}(k)/q_1^2q_2$$

证明：假设敌手 $\mathcal{A}_{\mathrm{II}}$ 可以破坏本文提出的方案，接下来构造算法 $\mathcal{B}_{II}$ 利用 $\mathcal{A}_{\mathrm{II}}$ 解决 CDH 困难问题。$\mathcal{B}_{II}$ 的输入为一个 CDH 实例 (g,g^a,g^b)，其任务就是要计算 g^{ab}。为了得到结果，$\mathcal{B}_{II}$ 利用 $\mathcal{A}_{\mathrm{II}}$ 作为子程序试图解决 CDH 困难问题，并且充当游戏中的挑战者。

首先 $\mathcal{B}_{II}$ 随机选取 $s\in\mathbb{Z}_q^*$，计算 $P_0=sP$，令 $params=\{q,G,G_T,e,P,P_0,H_1,H_2,l\}$，$msk=s$，将 $params$ 和 msk 发给敌手 $\mathcal{A}_{\mathrm{II}}$，$\mathcal{B}_{II}$ 随机选取 $M,N\in\{1,2,\cdots,q_1\}$。$\mathcal{A}_{\mathrm{II}}$ 进行一系列的询问，$\mathcal{B}_{II}$ 作出如下应答：

(1) H_1 询问：$\mathcal{B}_{II}$ 用表 L_1 来记录 $\mathcal{A}_{\mathrm{II}}$ 对 H_1 的询问。如果表 L_1 中已存在表项 $(ID,d_{ID},d_{ID}P)$，则 $\mathcal{B}_{II}$ 将 $d_{ID}P$ 返回给 $\mathcal{A}_{\mathrm{II}}$；若不存在，则随机选取 $d_{ID}\in\mathbb{Z}_q^*$，将 $(ID,d_{ID},d_{ID}P)$ 存入 L_1 中，并将 $d_{ID}P$ 返回给 $\mathcal{A}_{\mathrm{II}}$。

(2) H_2 询问：$\mathcal{B}_{II}$ 用表 L_2 来记录 $\mathcal{A}_{\mathrm{II}}$ 对 H_2 的询问。如果表 L_2 中已存在表项 (K_1,K_2,K_3,K)，则 $\mathcal{B}_{II}$ 将 K 返回给 $\mathcal{A}_{\mathrm{II}}$；若不存在，则随机选取 $K\in\{0,1\}^l$，将 (K_1,K_2,K_3,K) 存入 L_2 中，并将 K 返回给 $\mathcal{A}_{\mathrm{II}}$。

(3)计算部分密钥：$\mathcal{A}_{\mathrm{II}}$ 可以利用 msk 运行“部分密钥生成”程序，获得任何用户的部分密钥 $(P_{ID}=H_1(ID),D_{ID}=sP_{ID})$，$\mathcal{B}_{II}$ 用表 L_{puk} 来记录 $\mathcal{A}_{\mathrm{II}}$ 计算的部分密钥 $(ID,(P_{ID},D_{ID}))$。

(4)秘密值询问：$\mathcal{B}_{II}$ 用表 L_s 来记录 $\mathcal{A}_{\mathrm{II}}$ 对秘密值的询问。如果表 L_s 中已存在表项 (ID,s_{ID})，则 $\mathcal{B}_{II}$ 将 s_{ID} 返回给 $\mathcal{A}_{\mathrm{II}}$；如果不存在且 $ID\in\{ID_M,ID_N\}$，则 $\mathcal{B}_{II}$ 退出；否则，$\mathcal{B}_{II}$ 随机选取 $s_{ID}\in\mathbb{Z}_q^*$，将 (ID,s_{ID}) 存入 L_s，并返回给 $\mathcal{A}_{\mathrm{II}}$。

(5)公钥询问：$\mathcal{B}_{II}$ 用表 L_{pk} 来记录用户的公私钥对。如果表 L_{pk} 中已存在表项 $(ID,(P_{ID},T_{ID}),\cdot)$，则 $\mathcal{B}_{II}$ 将 (P_{ID},T_{ID}) 返回给 $\mathcal{A}_{\mathrm{II}}$；若不存在，则分为如下 3 种情况进行应答：

- 若 $ID\notin\{ID_M,ID_N\}$，则查询表 L_{puk} 得到 (P_{ID},D_{ID})，然后随机选取 $s_{ID}\in\mathbb{Z}_q^*$，计算 $T_{ID}=s_{ID}P$，将 $(ID,(P_{ID},T_{ID}),(s_{ID},D_{ID}))$ 存入 L_{pk} 中，并将 (P_{ID},T_{ID}) 返回给 $\mathcal{A}_{\mathrm{II}}$；
- 若 $ID=ID_M$，先查询表 L_{puk} 得到 (P_M,D_M)，令 $T_M=U=uP$，将 $(ID_M,(P_M,T_M),(\perp,D_M))$ 存入 L_{pk} 中，并将 (P_M,T_M) 返回给 $\mathcal{A}_{\mathrm{II}}$；
- 若 $ID=ID_N$，先查询表 L_{puk} 得到 (P_N,D_N)，令 $T_N=V=vP$，将 $(ID_N,(P_N,T_N),(\perp,D_N))$ 存入 L_{pk} 中，并将 (P_N,T_N) 返回给 $\mathcal{A}_{\mathrm{II}}$。

(6)私钥询问：若 $ID\notin\{ID_M,ID_N\}$，则 $\mathcal{B}_{II}$ 退出。否则，如果表 L_{pk} 中不存在表项 $(ID,(P_{ID},T_{ID}),(s_{ID},D_{ID}))$，则先如上运行公钥询问，然后在 L_{pk} 中查询 ID 的私钥 (s_{ID},D_{ID})，并将 (s_{ID},D_{ID}) 返回给 $\mathcal{A}_{\mathrm{II}}$。

(7)共享密钥询问：若 $(ID_A,ID_B)=(ID_M,ID_N)$，则 $\mathcal{B}_{II}$ 退出；否则，有 $|\{ID_A,ID_B\}\cap\{ID_M,ID_N\}|\leqslant 1$，不妨假设 $ID_A\notin\{ID_M,ID_N\}$，那么查询 L_{pk} 找到 ID_A 的私钥或通过私钥提取计算出 ID_A 的私钥 (s_A,D_A)、公钥 (P_A,T_A) 和 ID_B 的公钥 (P_B,T_B)，然后计算 $K_{A,B}$，记录 $(ID_A,ID_B,K_{A,B})$，并将 $K_{A,B}$ 返回给 $\mathcal{A}_{\mathrm{II}}$。

(8)测试询问：$\mathcal{A}_{\mathrm{II}}$ 选取一对 (ID_1,ID_2) 进行测试询问。如果 $(ID_1,ID_2)\neq(ID_M,ID_N)$，则 $\mathcal{B}_{II}$ 退出并且失败；否则，随机选取 $K'_{1,2}\in\{0,1\}^l$ 发送给 $\mathcal{A}_{\mathrm{II}}$。

至此，$\mathcal{B}_{\mathrm{II}}$ 的模拟结束。$\mathcal{A}_{\mathrm{II}}$ 若输出 $b'=1$，则 $\mathcal{B}_{II}$ 从 L_2 中随机选取 (K_1,K_2,K_3)，$\mathcal{B}_{II}$ 输出 K_2。

下面分析 $\mathcal{B}_{\mathrm{II}}$ 成功的概率。

设 $\mathcal{G}$ 表示事件“$\mathcal{B}_{II}$ 在模拟过程中不退出”，则 $\Pr[\mathcal{G}]\geqslant 1/q_1^2$。综上，如果 $\mathcal{B}_{II}$ 在模拟过程中不退出，且 $\mathcal{A}_{\mathrm{II}}$ 对 (K_1,K_2,K_3) 进行过 H_3 询问，其中 $K_2=s_AT_B=uvP$，那么 $\mathcal{B}_{\mathrm{II}}$ 就可以以优势 $Adv_{\mathcal{A}_{\mathrm{II}}}^{CDH}$ 解决 *CDH* 问题，且

$$Adv_{\mathcal{A}_{\mathrm{II}}}^{CDH}=\Pr[\mathcal{G}]\cdot Adv_{\mathcal{A}_{\mathrm{II}}}(k)/q_2\geqslant Adv_{\mathcal{A}_{\mathrm{II}}}(k)/q_1^2q_2$$

5 性能分析

本节将对本文提出的无证书非交互密钥交换协议与文献[13,14]以及文献[19]中的方案进行安全性和效率方面的比较。在安全性方面，主要从是否存在密钥托管问题和是否允许部分秘密泄露两个方面进行衡量。在计算代价方面，我们从用户注册、用户计算共享密钥以及中心的计算代价 3 个方面对协议进行分析。由于双线性对运算和标量乘法运算是协议中计算代价最高的运算，因此仅考虑双线性对运算（用 P 表示）和标量乘法运算（用 S 表示），结果如表 1 所列。

表 1 性能比较

协议	密码体制	安全性		效率		
		密钥托管安全	允许部分秘密泄露	用户注册	用户计算共享密钥	中心
SOK 协议[13]	ID-PKC	否	否	无	1P	1S
Dupont 和 Enge 协议[14]	ID-PKC	否	否	无	2P	2S
Wu 和 Lin 协议[19]	Self-Certified PKC	否	否	1S+2P	1P	3S
本文协议	CL-PKC	是	是	1S	2P+2S	1S

在计算代价方面，从表 1 可见，对于中心的计算量，所提协议和 SOK 协议[13]一样，只有一个标量乘法运算。但是，对于用户的计算量，由于用户在注册阶段不需要验证中心分发的密钥对，只需进行一个标量乘法运算，因此所提协议比 Wu 和 Lin 协议[19]少两个对运算；在计算共享密钥时，我们的协议中有两个对运算和两个标量乘法运算，比其他 3 个协议计算量都大。但应注意到，大部分的计算代价来自于解决密钥托管问题以及实现更高的安全性，因此这样的计算代价是可以接受的。

（下转第 111 页）

先构建网络潜质入侵数学演化模型，采用经验模态分解方法对高频分量进行滤波处理，去除虚假分量，通过递阶控制调整HHT频谱偏移，使检测的入侵信号特征的组成成分形成最佳匹配，采用HHT谱偏移量递阶控制策略，抑制了包络线失真引起的边界控制误差，抑制了频谱泄漏，提高了检测性能。研究结果表明，改进的HHT检测算法能有效检测出信噪比极低背景下的信号特征，对诸如ipsweep和smurf等干扰性极强的潜在入侵信号具有较好的检测效果，检测性能较传统方法提高显著。研究成果在网络安全防御和对抗等领域具有较好的应用价值。

参 考 文 献

[1] 孙言强，王晓东，周兴铭. 无线网络中的干扰攻击[J]. 软件学报，2012，23(5)：1207-1221

[2] 周华，周海军，马建锋. 基于博弈论的入侵容忍系统安全性分析模型[J]. 电子与信息学报，2013，35(8)：1933-1939

[3] 梁力. 一种网络多次变异信息入侵检测算法[J]. 科技通报，2012，10(28)：55-57

[4] Bimal K M，Gholam M A. Differential epidemic model of virus and worms in computer network [J]. International Journal of Network Security，2012，14(3)：149-155

[5] 樊爱宛，时合生. 基于特征选择和SVM参数同步优化的网络入侵检测[J]. 北京交通大学学报，2013，37(5)：58-61

[6] Li Hong，Qian Chang-ji，Sun Li-zhen，et al. Simulation of a flexible polymer tethered to a flat adsorbing surface [J]. Journal of Applied Polymer Science，2012，124：282-287

[7] 罗柏文，沈彩耀，于宏毅. 采用余弦调制滤波器组的多径衰落信号子带合成[J]. 信号处理，2013，29(5)：537-543

[8] 葛海慧，肖达，陈天平，等. 基于动态关联分析的网络安全风险评估方法[J]. 电子与信息学报，2013，35(11)：2630-2636

[9] 张宗飞. 基于量子进化算法的网络入侵检测特征选择[J]. 计算机应用，2013，33(5)：1357-1361

[10] Zhu Q Y，Yang X F，Yang L X，et al. Optimal control of computer virus under a delayed model [J]. Applied Mathematics and Computation，2012，218(23)：11613-11619

[11] 张辉. 自体集网络入侵检测中的高效寻优算法仿真[J]. 计算机仿真，2013，30(8)：297-300

[12] 林冬茂，薛德黔. 一种基于无监督免疫优化分层的网络入侵检测算法[J]. 计算机科学，2013，40(3)：180-182

[13] 叶竞，石锐，何庆华. 基于HHT和改进CSP算法的运动想象BCI系统[J]. 重庆理工大学学报：自然科学版，2012，26(5)：70-73

(上接第106页)

结束语 本文提出了一种基于无证书公钥密码体制的非交互密钥交换协议，给出了这类协议的定义并刻画了协议的安全模型，然后给出了一种利用双线性对的无证书非交互密钥交换协议的构造方案，而且还在随机预言模型下基于BDH困难问题给出了该方案的安全性证明。该方案解决了基于身份的非交互密钥交换协议中的密钥托管问题。另外，该协议可以抵抗无证书公钥密码体制中的两类敌手的攻击，允许部分秘密信息泄露，因此其比现有的非交互密钥交换协议具有更高的安全性。

参 考 文 献

[1] Dodis Y，Katz J，Smith A，et al. Composability and on-line deniability of authentication[M]// Theory of Cryptography. Berlin，Springer Berlin Heidelberg，2009：146-162

[2] Boyd C，Mao W，Paterson K G. Key agreement using statically keyed authenticators[C]// Second International Conference，ACNS 2004，Yellow Mountain，China，2004：248-262

[3] Jakobsson M，Sako K，Impagliazzo R. Designated verifier proofs and their applications [C] // International Conference on the Theory and Application of Cryptographic Techniques. Saragossa，1996：143-154

[4] Diffie W，Hellman M. New directions in cryptography[J]. IEEE Transactions on Information Theory，1976，22(6)：644-654

[5] Bernstein D J. Curve25519：new Diffie-Hellman speed records [C]// 9th International Conference on Theory and Practice in Public-Key Cryptography. New York，2006：207-228

[6] Cash D，Kiltz E，Shoup V. The twin Diffie-Hellman problem and applications[M]// Advances in cryptology-EUROCRYPT 2008. Berlin，Springer Berlin Heidelberg，2008：127-145

[7] Freire E S V，Hofheinz D，Kiltz E，et al. Non-interactive key exchange [M] // Public-Key Cryptography-PKC 2013. Berlin，Springer Berlin Heidelberg，2013：254-271

[8] Boneh D，Zhandry M. Multiparty key exchange，efficient traitor tracing，and more from indistinguishability obfuscation [R]. Cryptology ePrint Archive，Report 2013/642，2013

[9] Maurer U M，Yacobi Y. Non-interactive public-key cryptography[M]// Advances in Cryptology-EUROCRYPT'91. Berlin，Springer Berlin Heidelberg，1991：498-507

[10] Lim C H，Lee P J. Modified Maurer-Yacobi's scheme and its applications[M]// Advances in Cryptology-AUSCRYPT'92. Berlin，Springer Berlin Heidelberg，1993：308-323

[11] Maurer U M，Yacobi Y. A non-interactive public-key distribution system[J]. Designs，Codes and Cryptography，1996，9(3)：305-316

[12] Maurer M，Kügler D. A note on the weakness of the Maurer-Yacobi squaring method [R]. Technical report，TI 15/99，TU Darmstadt，1999

[13] Sakai R，Ohgishi K，Kasahara M. Cryptosystems based on pairings[C]// The 2000 Symposium on Cryptography and Information Security. Okinawa，2000：26-28

[14] Dupont R，Enge A. Provably secure non-interactive key distribution based on pairings[J]. Discrete Applied Mathematics，2006，154(2)：270-276

[15] Paterson K G，Srinivasan S. On the relations between non-interactive key distribution，identity-based encryption and trapdoor discrete log groups[J]. Designs，Codes and Cryptography，2009，52(2)：219-241

[16] Freire E S V，Hofheinz D，Paterson K G，et al. Programmable Hash Functions in the Multilinear Setting? [M]// Advances in Cryptology-CRYPTO 2013. Berlin，Springer Berlin Heidelberg，2013：513-530

[17] Steinwandt R，Corona A S. Identity-based non-interactive key distribution with forward security[J]. Designs，Codes and Cryptography，2012，64(1/2)：195-208

[18] Lin X J，Ren Ran，Wei Z G，et al. Comment on "Identity-based non-interactive key distribution with forward security"[J]. Designs，Codes and Cryptography，2013：1-7

[19] Wu T S，Lin H Y. Non-Interactive Authenticated Key Agreement over the Mobile Communication Network[J]. Mobile Networks and Applications，2013，18：594-599